Identifying objects – the ASN.1 approach

John Larmouth
ISO and ITU-T ASN.1 Rapporteur

j.larmouth@salford.ac.uk

Study Group 17
ASN.1

Note, for best viewing, this presentation needs the Dom Casual and Brush Script fonts.

Speakers preamble notes

- (SE)X-rated. Leave now, or shut me up.
- Olivier Dubuisson or Phil Griffin might be better presenters.
- But I was part of the Blood Spilling in 1985: Verbose characters or computer-friendly numerics; new RA or re-use existing ones.
- Everyone likes their own identification scheme (particularly in the MoU!). I am NOT selling ASN.1 OIDs as the universal solution for everything, but they ARE used and useful.
- Dry, boring, not sexy and very simple, with not much to say!

Why the rainbow?

- An infinity of colours
- A secondary rainbow (did you see it?)
- Others to an infinity of internal reflections
- Not really relevant, but it is a nice picture!
- But an infinity of arcs and an infinity of depth is what OIDs are about

The ASN.1 approach to identification

- One of many, many approaches
- Is basically very simple
- Has proved useful in many environments
- Can be used without using ASN.1
- Unfortunately, it is hard to present it in a sexy way!

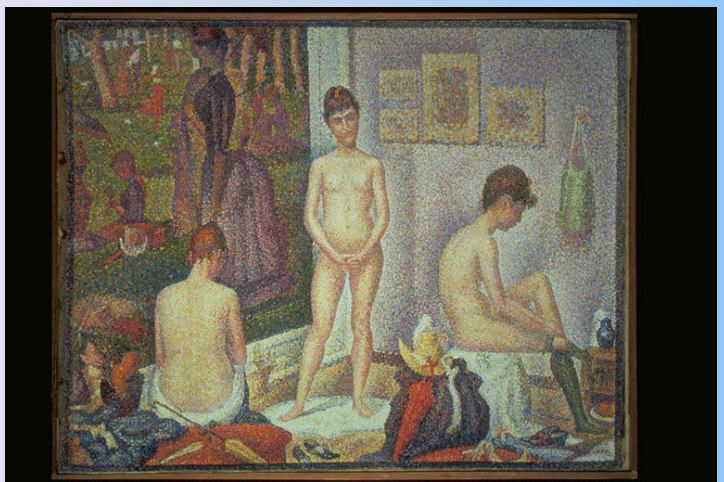
But I will try!

There are many approaches to object identification

- Bar codes are well known
- IP addresses are a binary form
- URLs are well-known
- URNs are less well-known
- NSAP addresses are unused today
- UUIDs are important too

What are the differences?

- Some are character-based, some are binary
- Some need central allocation, others have various levels of hierarchy
- Some are fixed length, others are variable length
- To some extent it is horses for courses
- They all are sisters!



Study Group 17
ASN.1

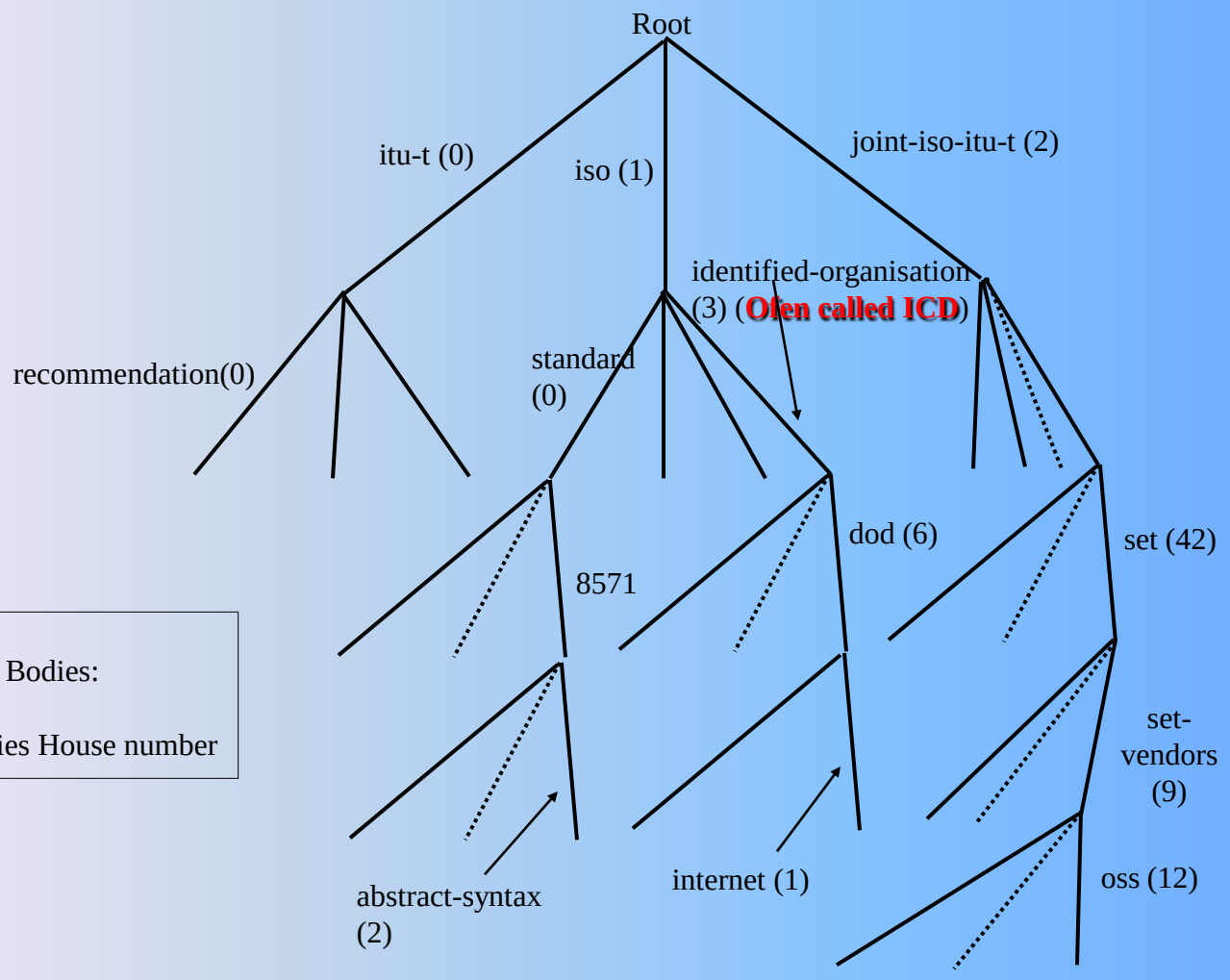
Are OIDs new to the MoU MG?

- No!
- Presented to the Geneva Business Objects Summit in November 2000 by William Lyons
- Banking.ppt

So .. What is the mechanism?

- A hierarchical structure of registration authorities
- An object identifier tree
- Arcs are numbered (zero to infinity)
- Infinitely many arcs from each node
- An RA allocates arcs beneath its node to subordinate RAs, and so on, to an infinite depth
- Objects are identified by the path from the root to a leaf (or intermediate node)

A small part of the OID tree – Get Hung!



ISO:
National Bodies:
BSI:
Companies House number

Study Group 17
ASN.1

Notations and encodings of OIDs

- **Very compact binary encoding (normally used in all computer comms except XML), see next slide**
- **Simplest character encoding (used for XML and other Internet protocols) is (for example)**

  1.0.8571.2.29
- **More readable (for human consumption) is**

  {iso standard 8571 abstract-syntax (2) pci (29) }
- **Or**

  {itu-t recommendation x 1081 pictures (0) leonardo (3)}

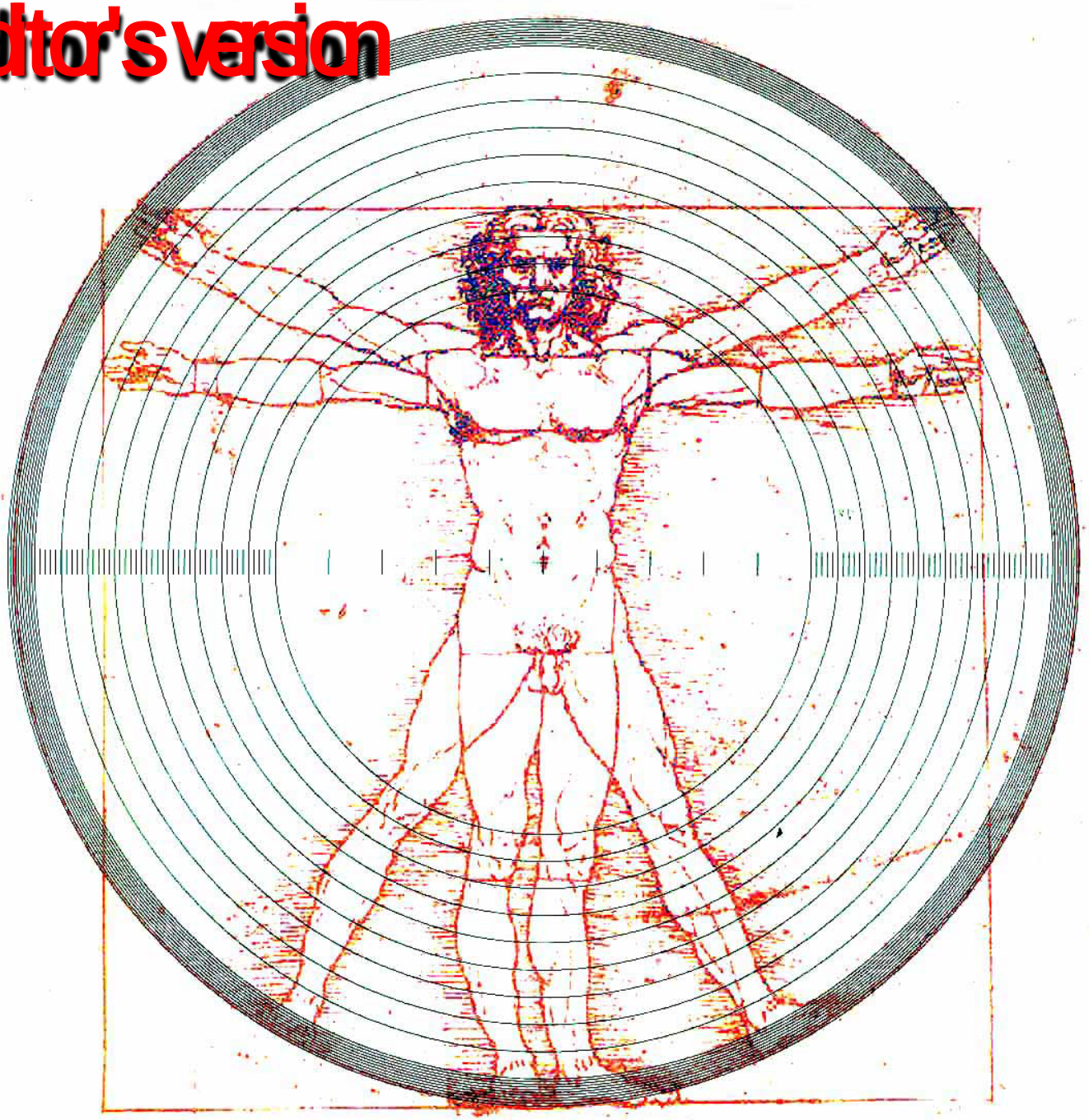
Picture follows!

The binary encoding

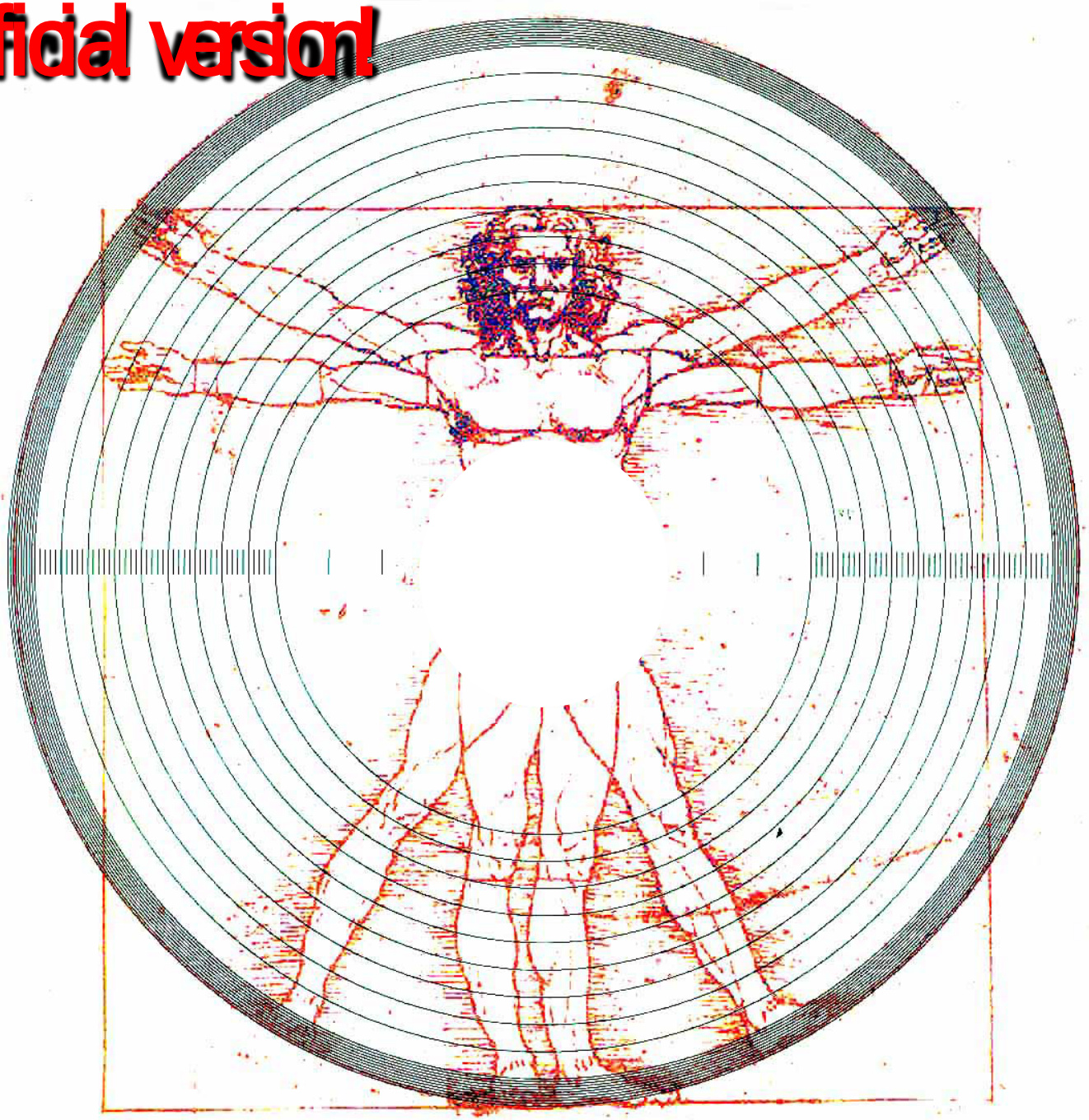
- Roughly one octet per component
- Uses bit 8 as a more bit
- Top two components handled specially
- {0 0} to {0 39} encodes into one octet only
- {1 0} to {1 39} encodes into one octet only
- {2 0} to {2 47} encodes into one octet only
- {2 48} on will use two or more octets

And now the picture!

The Editor's version



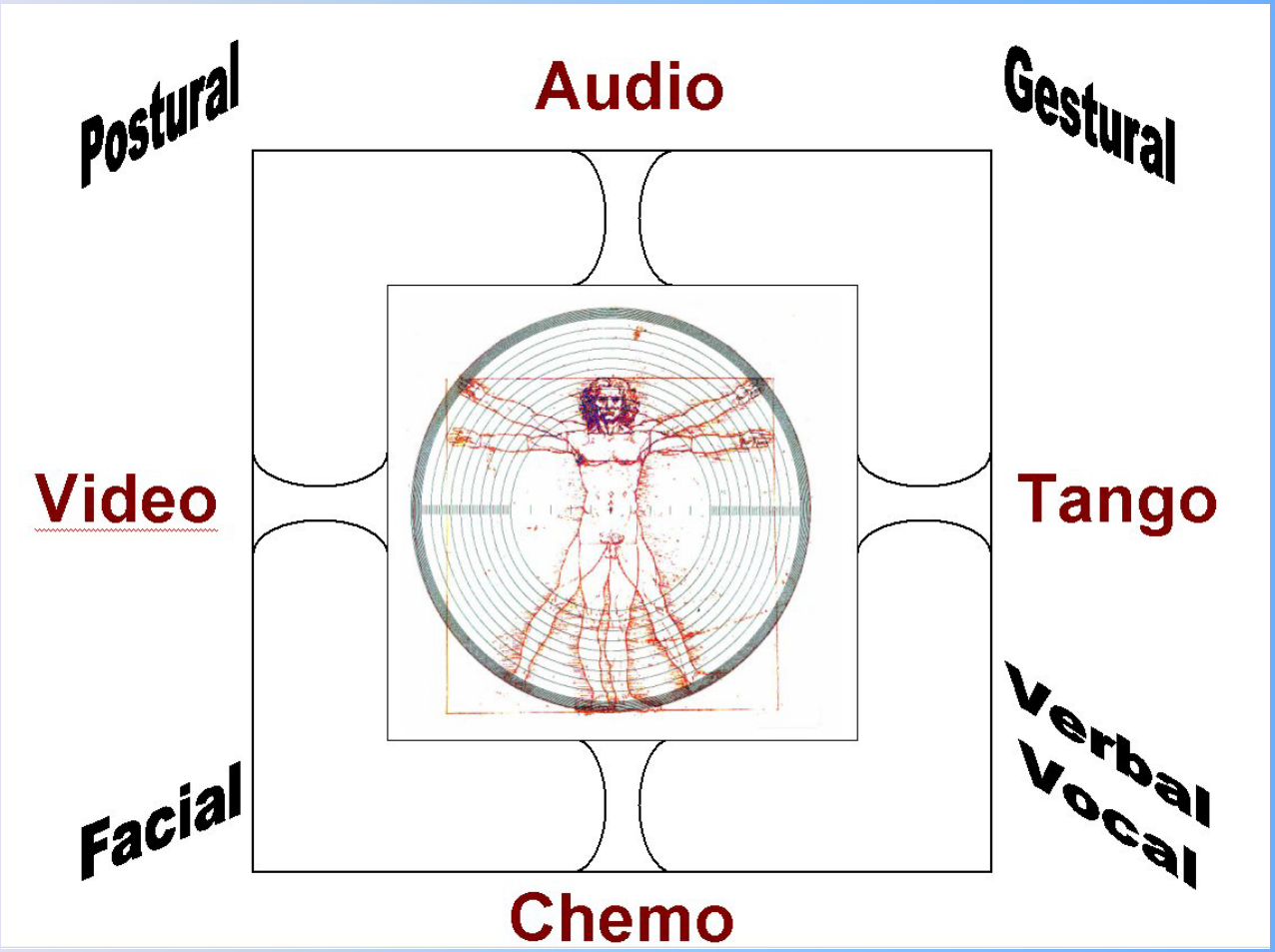
The official version!



But let's see the (two) videos!

- Not much to do with ASN.1 Object Identifiers, but I think interesting!
- Part of the work of ITU-T SG17
- First an introduction by Leonardo himself, then a review of the Recommendation
- (Click on the black display to start the video, and when finished click outside the video area to move to the next slide)

But one more picture first



Study Group 17
ASN.1

Back to OIDs again!

- **Here is an OASIS of tranquillity:**

  {oasis (2) tech-committees (45)
  xcbf(20) standard (0) version (2002)}

  or 2.45.20.0.2002

  or <xxx xmlns="urn:oid:2.45.20.0.2002">…<\xxx>

Artificial – not applied for yet!

Study Group 17

Try another!

- **Facilitation of trade:**

  {un-cefact(2) edi(50) invoice(0) version-2004(2) }

  or 2.50.0.2

  or <xxx xmlns="urn:oid:2.50.0.2">…<\xxx>

Artificial – not applied for yet!

Study Group 17

A real one

- **Face recognition:**

  {iso standard 19794 part(5) version(1) }

  or 1.0.19794.5.1

  or <xxx xmlns="urn:oid:1.0.19794.5.1">…<\xxx>

Study Group 17
ASN.1

ITU-T TSAG Recommendation

- **Was requested to devise a uniform approach for XML namespace specification across all ITU-T Recommendations**
- **Asked SG17 for advice**
- **Was advised to recommend the use of the form:**

<xxx xmlns="urn:oid:0.0.6. ….">…<\xxx>

What about UUIDs?

- Universally unique identifiers
- Verbose – 128 bits (but only = 16 chars)
- ISO/IEC 9834-8 | ITU-T Rec X.667
- Can self-generate OIDs at the rate of about 10 million per second
- Unambiguous over the next 2000 years
- Can optionally register them
- OID is 2.25.xxx…..

Time for another picture!
OIDs provide levels in levels

Study Group 17
ASN.1

All very good, but are they used?

- Not really very much? Depends on comparators!
- Only 59,000 known to be allocated! Certainly many more in reality.
- Telephone numbers will do better!
- But in their field, OIDs have had a pretty good take-up
- See http://oid.elibel.tm.fr

Security algorithm uses of OIDs

- This is one area where OIDs are universally used.
- Use a Digital Certificate, and you use an OID.
  - Secure Hash Algorithm 2 (SHA2)
    { joint-iso-itu-t(2) country(16) us(840)
    organization(1) gov(101)
    csor(3) nistAlgorithm(4) hashAlgs(2)
  - RSA Encryption
    { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) 1 1 }

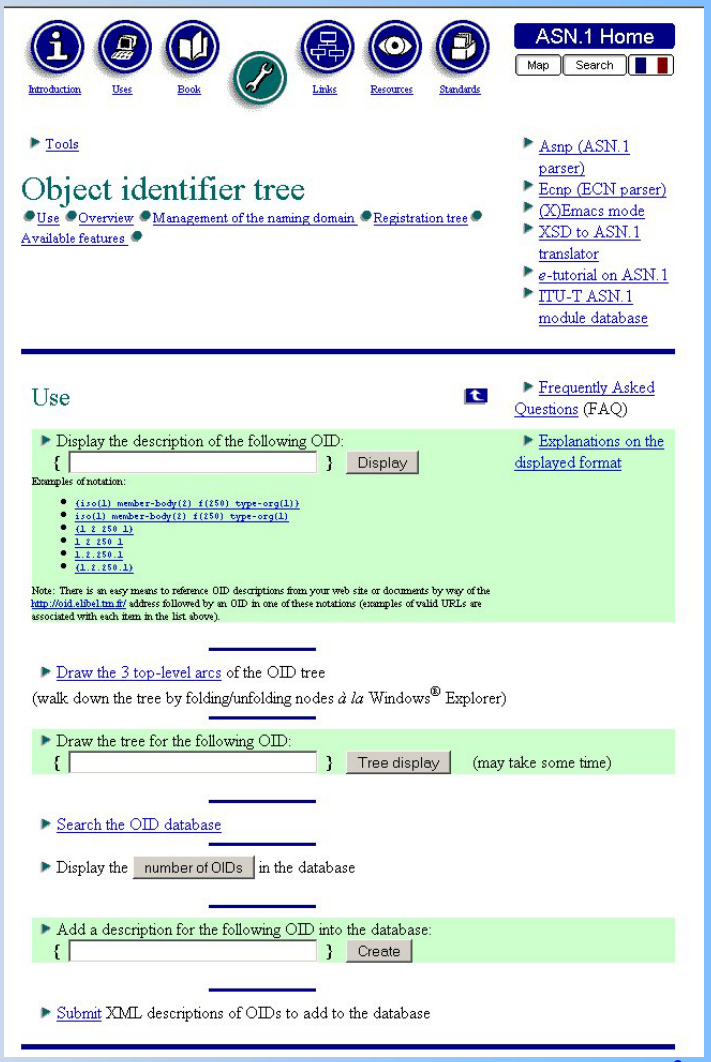
Other areas

- Many ITU-T Recommendations
- Biometrics and other ISO Standards
- Many US ANSI X.9 specifications
- US Banking specifications
- UPU and international carrier parcel tracking
- 3GPP Mobile phones
- Not as widespread as bar-codes, but heavily used in computer communications protocols

Web support

- Go to http://oid.elibel.tm.fr
- Number of OIDs
- Details about an OID
- Provide details about a (new) allocation of an OID
- Much additional information

The Elibel OID page



Introduction | Uses | Book | Links | Resources | Standards

ASN.1 Home

Map | Search

▶ Tools

Object identifier tree

Use • Overview • Management of the naming domain • Registration tree • Available features •

- Asnp (ASN.1 parser)
- Ecnp (ECN parser)
- (X)Emacs mode
- XSD to ASN.1 translator
- *e*-tutorial on ASN.1
- ITU-T ASN.1 module database

Use

▶ Frequently Asked Questions (FAQ)

▶ Display the description of the following OID:
{ } Display

▶ Explanations on the displayed format

Examples of notation:

- {iso(1) member-body(2) f(250) type-org(1)}
- iso(1) member-body(2) f(250) type-org(1)
- {1 2 250 1}
- 1 2 250 1
- 1.2.250.1
- {1.2.250.1}

Note: There is an easy means to reference OID descriptions from your web site or documents by way of the http://oid.elibel.tm.fr/ address followed by an OID in one of these notations (examples of valid URLs are associated with each item in the list above).

▶ Draw the 3 top-level arcs of the OID tree
(walk down the tree by folding/unfolding nodes *à la* Windows® Explorer)

▶ Draw the tree for the following OID:
{ } Tree display (may take some time)

▶ Search the OID database

▶ Display the number of OIDs in the database

▶ Add a description for the following OID into the database:
{ } Create

▶ Submit XML descriptions of OIDs to add to the database

Study Group 17
ASN.1

Near Futures

- Web services (SOAP and all that) support to register or obtain UUID-based OIDs
- Fast Web services support
- Courtesy of the ITU-T TSB, France Telecom, Sun Microsystems, and OSS Nokalva

Requests for top-level allocations

- Formally, contact the ITU-T TSB or ISO/IEC SC6 Secretariat, for the attention of the ASN.1 Rapporteur, in both cases.
- Informally, contact j.larmouth@salford.ac.uk

MoU MG Recommendations?

- ASN.1 object identifiers should be considered alongside other existing identification mechanisms, particularly when there is a need for:
  - simple globally unambiguous identification
  - allocation of identifiers by many organizations
  - hierarchical not centralized allocation mechanisms
  - compact binary encodings of the ID
- MoU member organizations should consider obtaining a top-level allocation (see the OASIS and UN/CEFACT examples above)

How to end?

- OIDs provide a standardised, distributed, low admin overhead, flexible, hierarchical system for object identification, with few restrictions
- They provide efficient binary, simple numeric, and human readable representations
- Is it too much to say that they are a shining light?

Study Group 17
ASN.1